AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Two Electronic Devices identified in Attachment A and located at 300 Arboretum Place Suite 500, Richmond, VA 23236

Case No. 3:19SW99 Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A, incorporated herein by reference.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18, U.S.C. § 656	Theft, embezzlement, or misapplication by bank officer or employee
18, U.S.C. § 472	Uttering counterfeit obligations or securities

The application is based on these facts:
See Attached Affidavit, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kyle Temple, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: March 13, 2019

/s/
David J. Novak
United States Magistrate Judge
Judge's signature

City and state: Richmond, VA

David J. Novak, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

IN THE MATTER OF THE SEARCH OF: **Black Dell Inspiron One 2020 Desktop, model W06B** **Blue Toshiba Laptop, model Satellite, S/N 6B351781W** **LOCATED AT: 300 Arboretum Place Suite 500, Richmond, VA 23236**	Case No. 3:19SW 99 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Kyle R. Temple, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices— which are currently in law enforcement possession and described in Attachment A. This application seeks the extraction from that property of electronically stored information described in Attachment B

2. I am a Special Agent with the United States Secret Service (USSS). I have been employed as a Special Agent since 2015, and I am currently assigned to the Office of Investigations, Richmond Field Office. As part of my current duties, I investigate criminal violations relating to financial crimes such as counterfeit currency, identity theft, bank fraud, wire fraud and conspiracy. I have participated in the preparation and presentation of arrest warrants and search warrants, and I am familiar with the methods of individuals who commit

offenses related to financial crimes and counterfeit currency. I, as a Special Agent under the Electronic Crimes Special Agent Program, have also been trained in computer forensics by the Treasury Computer Forensics Training Program. I was previously employed as a Uniformed Officer for the USSS in Washington D.C. for approximately 5 years.

3. As a Special Agent with the USSS, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Titles 18, U.S.C. § 656 & 18, U.S.C. § 472 have been committed by Jorge Omar Navarro, hereinafter "NAVARRO". There is also probable cause to believe that the property described in Attachment A has been used in furtherance of these crimes. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

RELEVANT STATUTES

5. *Theft, embezzlement, or misapplication by bank officer or employee,* Title 18, U.S.C. § 656, provides that "whoever, being an officer, director, agent or employee of, or connected in any capacity with any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, branch or agency of a foreign bank, or organization operating under section 25 or section 25(a) [1] of the Federal Reserve Act, or a receiver of a national bank, insured bank, branch, agency, or organization or any agent or employee of the receiver, or a Federal Reserve Agent, or an agent or employee of a Federal Reserve Agent or of the Board of Governors of the Federal Reserve System, embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of such bank, branch, agency, or organization or holding company or any moneys, funds, assets or securities

entrusted to the custody or care of such bank, branch, agency, or organization, or holding company or to the custody or care of any such agent, officer, director, employee or receiver, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both; but if the amount embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both."

6. *Uttering counterfeit obligations or securities*, Title 18 U.S.C. § 472, provides that "whoever, with intent to defraud, passes, utters, publishes, or sells, or attempts to pass, utter, publish, or sell, or with like intent brings into the United States or keeps in possession or conceals any falsely made, forged, counterfeited, or altered obligation or other security of the United States, shall be fined under this title or imprisoned not more than 20 years, or both.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The property to be searched is described below and in Attachment A:

(a) Black Dell Inspiron One 2020 Desktop computer, model #W06B (hereinafter referred to as "DEVICE 1")

(b) Blue Toshiba Laptop Computer, serial #6B351781W (hereinafter referred to as "DEVICE 2")

8. The devices are currently located at USSS Richmond Field Office, located at 300 Arboretum Place Suite 500, Richmond, VA 23236.

9. The applied-for warrant would authorize the forensic examination of DEVICES 1 & 2, for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

10. The statements contained in this affidavit are based in part on: information provided by written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; the results of physical and electronic surveillance conducted by law enforcement agents; and my experience, training and background as a Special Agent with the USSS. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

11. On September 10, 2018, Danville Police Department (DPD) Officer Darnell responded to the United Rubber Workers Community Federal Credit Union (URWFCU), at 142 S Main St, Danville VA 24541, in reference to a theft. On scene Officer Darnell spoke with branch manager, A.J., who stated the Head Teller, NAVARRO (cellular #434-709-9759), texted URWFCU CEO, C. D. (cellular #434-203-8868), the morning of September 10, 2018, stating that he had taken $600,000 from the vault in the bank and had left the area. Additionally, NAVARRO's text stated that he took all the genuine hundred dollar Federal Reserve Notes (FRN) bundles from the vault, left the top and bottom FRNs within the bundle, and replaced all the other genuine FRNs with counterfeit (CFT) FRNs in between the top and bottom genuine FRNs.

12. On September 10, 2018, DPD Detective Abbott met with C.D. at 142 S Main St, Danville VA 24541 in reference to the theft/embezzlement. C.D. stated that she received a text message from NAVARRO at approximately 0200 on September 10, 2018 stating he had taken $600,000 from the bank vault and replaced it with counterfeit currency. C.D. stated she opened

the bank vault later that morning and found multiple bundles of $100 FRNs, had been opened, replaced, and resealed in the appearance of legitimate bundles received from the Federal Reserve. Upon closer examination of these bundles, it became clear that although there was a $100 FRN on the top and the bottom of each bundle, the remainder of each bundle was filled with $100 CFT FRNs with the caption "For Motion Picture Purposes" displayed on them. Total reported loss at this location and time was $521,670. C.D. reported that NAVARRO was the Head Teller at the above location.

13. Additionally on September 10, 2018, E.H., reported that $72,000 ($22,000 in $50 FRNs; $50,000 in $100 FRNs) were found to be missing from the vault at the Arnett branch of URWFCU located at 539 Arnett Blvd, Danville, VA 24540. The money was verified in the vault on Friday September 7, 2018 at closing. NAVARRO was confirmed to have been working at this branch on Saturday September 8, 2018 as a teller and assisting with closing the branch.

14. On September 10, 2018, DPD obtained a felony arrest warrant for NAVARRO for embezzlement of greater than $500. On September 11, 2018, DPD obtained a search warrant for NAVARRO's residence at 625 Park Avenue Danville, VA 24540, which the affiant assisted with the execution. During the search, DEVICE 2 was seized pursuant to the search warrant in NAVARRO's residence, along with purple money bands ($2000 amounts, the same used at URWFCU).

15. On September 14, 2018, Detective Abbott obtained video surveillance footage of the Arnett branch for Saturday September 8, 2018. The footage showed NAVARRO taking money from the vault on Saturday September 8, 2018. Video surveillance footage of the 142 Main St. branch was also obtained, showing NAVARRO entering the branch in the middle of the night on Saturday September 8, 2018 at approximately 0148 hours. Footage shows NAVARRO taking

money out of the vault and leaving the branch with what appears to be money around approximately 0202 hours.

16. On September 11, 2018, URWFCU employee L.F. , reported to DPD that NAVARRO had used a URWFCU owned desktop computer (DEVICE 1), located at the 142 S. Main St. branch, for personal email/internet use and had left all accounts he last used open on DEVICE 1. L.F. advised that NAVARRO's past electronic actions, including reserving a room at the Ritz-Carlton Hotel in Charlotte, NC on September 08, 2018 and placing order for "prop money" were still visible on DEVICE 1. DPD confirmed with the Ritz-Carlton Hotel in Charlotte, NC that NAVARRO checked into their location on September 8, 2018 and checked out on September 9, 2019. In addition they stated that NAVARRO arrived in a black Porsche. In addition, L.F. advised that DEVICE 1 contained possible information pertaining to NAVARRO's potential location, Guadalajara, Mexico.

17. DEVICES 1 & 2 are currently in the lawful possession of the USSS. They came into the USSS's possession in the following way: taken during the execution of a warrant by DPD and custody turned over to the USSS in connection with USSS investigation of violations, by NAVARRO, of Title 18 U.S.C. § 656 & § 472. The items to be searched for and seized under this warrant are described more particularly in Attachment B.

18. In my training and experience, I know that the DEVICES 1 & 2 have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when DEVICES 1 & 2 first came into the possession of the USSS.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

b. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Log Files: Are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Probable cause*. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how DEVICES 1 & 2 were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES 1 & 2 because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of DEVICES 1 & 2 consistent with the warrant. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of DEVICES 1 & 2 to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine DEVICES 1 & 2 already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a warrant to search DEVICES 1 & 2 described in Attachment A and seize the items described in Attachment B. I respectfully request that this Court issue a search warrant for DEVICES 1 & 2, authorizing the seizure and search of the items described in Attachment B.

REQUEST FOR SEALING

26. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminals as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other criminals online as they deem appropriate, i.e., post them publicly online through the forums. Premature disclosure of the contents of this affidavit and related

documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Special Agent Kyle R. Temple
United States Secret Service

Subscribed and sworn to before me this 13th day of March, 2019.

/s/
David J. Novak
United States Magistrate Judge

Honorable David J. Novak
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

IN THE MATTER OF THE SEARCH OF:
Black Dell Inspiron One 2020 Desktop, model W06B

Blue Toshiba Laptop, model Satellite, S/N 6B351781W

LOCATED AT: 300 Arboretum Place Suite 500, Richmond, VA 23236

Case No. 3:19sw99

Filed Under Seal

ATTACHMENT A

1. The property to be searched described below and in Attachment A:

(a) Black Dell Inspiron One 2020 Desktop computer, model #W06B (hereinafter referred to as "DEVICE 1")

(b) Blue Toshiba Laptop Computer, serial #6B351781W (hereinafter referred to as "DEVICE 2")

2. The devices are currently located at USSS Richmond Field Office, located at 300 Arboretum Place Suite 500, Richmond, VA 23236.

3. This warrant authorizes the forensic examination of DEVICES 1 & 2 for the purpose of identifying the electronically stored information described in Attachment B.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

IN THE MATTER OF THE SEARCH OF:
Black Dell Inspiron One 2020 Desktop, model W06B

Blue Toshiba Laptop, model Satellite, S/N 6B351781W

LOCATED AT: 300 Arboretum Place Suite 500, Richmond, VA 23236

Case No. 3:19sw99

Filed Under Seal

ATTACHMENT B

EVIDENCE TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, U.S.C., Sections § 656 & § 472.

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. electronically stored data, files, or digital information relating to violations of Title 18, U.S.C., Sections § 656 & § 472.

c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

f. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

i. evidence of the times the COMPUTER was used;

j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

l. records of or information about Internet Protocol addresses used by the COMPUTER;

m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

n. contextual information necessary to understand the evidence described in this attachment.

o. any information recording NAVARRO's schedule or travel;

p. all bank records, checks, credit card bills, account information, and other financial records.

3. Records, information, and items relating to violations of the statutes described above including

   a. Records, information, and items relating to the ownership or use of computer equipment found in 625 Park Avenue Danville, VA, including sales receipts, bills for Internet access, and handwritten notes;

   b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

4. Records evidencing the use of the Internet Protocol address to communicate with [[Yahoo! mail servers, Instagram, SnapChat, Twitter, and Facebook servers]], including:

   a. records of Internet Protocol addresses used;

5. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, laptop computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.